тения потребителей существуют различные инструменты. Одним из самых актуальных является АВС-анализ (рейтинговый анализ продаж). АВС-анализ проводится для определения фокуса расстановки приоритетов супермаркета в продажах.

Только тщательный комплексный анализ всей информации из этих отчетов, может дать основание для принятия управленческих решений и совершения различных управленческих действий руководителем супермаркета розничной торговли.

Т. М. Тардаскіна, аспірантка, викл.,
каф. маркетингу та менеджменту
ОНАЗ ім. О. С. Попова, м. Одеса

ОЦІНКА РИЗИКІВ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Телекомунікаційні мережі стали невід'ємною частиною інформаційно-комунікаційних технологій (ІКТ), які перетворюються у фундамент економіки, його бюджетно та системно утворюючий рушій. У той же час, як будь-яке явище прогресу, розвиток ІКТ несе за собою нові проблеми, нові ризики, нові побічні негативні явища, зокрема проблему інформаційної безпеки. Незважаючи на своє вирішальне значення для розвитку інформаційного суспільства, ІКТ виявилися слабо захищеними від зловживань, зовнішніх вторгнень, стали ареною діяльності кіберзлочинців і розвитку кібертероризму. Одним з дієвих способів вдосконалення систем інформаційної безпеки є визначення та страхування ризиків.

Під ризиком інформаційної безпеки розуміють потенційну можливість того, що загрози будуть використовувати вразливості інформаційних ресурсів і таким чином спричиняти шкоду підприємству. Ризик оцінюється як функція імовірності та міри величини наслідків таких подій. У ряді випадків не існує прямих шкал для виміру певних властивостей, таких як цінність захищаємої інформації або інформаційного ресурсу, що захищаються. Тоді можуть застосовуватись похідні шкали, такі як вартість та тривалість відновлення ресурсу тощо. Часто застосовують шкали для отримання експертної оцінки, наприклад, які мають три значення: малоцінний інформаційний ресурс, який може бути відновлений швидко і дешево; ресурс середньої цінності, який може бути відновлений за час, не більший за критичний, а вартість його відновлення висока;

цінний ресурс, від якого залежать критично важливі задачі, у випадку втрати якого час на відновлення перевищує критичний або вартість відновлення якого надзвичайно висока.

При оцінці ризиків необхідно враховувати суб'єктивну точку зору власника інформаційних ресурсів, організаційні та психологічні аспекти. У простих випадках використовують оцінку ризиків по двом факторам, яка виражається формулою [1]:

$$\text{РИЗИК} = \text{Р}_{\text{загрози}} \times \text{ВАРТІСТЬ ВТРАТ}.$$

Тобто ризик — це оцінка математичного очікування втрат. Можливо застосування методики оцінки ризику по трьом факторам — загрозам, вразливостям і вартості втрат. Загрозою називають сукупність умов та факторів, які можуть стати причиною порушення цілісності, доступності, конфіденційності інформації. Вразливість — це слабкість у системі захисту, яка робить можливою реалізації загрози. У цій методиці ризик визначається так:

$$\text{РИЗИК} = \text{Р}_{\text{загрози}} \times \text{Р}_{\text{вразливості}} \times \text{ВАРТІСТЬ ВТРАТ}.$$

Цей вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загального принципу, якщо хоча б одна з шкал є якісною.

У доповіді розглядається класифікація, оцінка та можливість і корисність страхування ризиків системи інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Петренко С., Симонов С.* Экономически оправданная безопасность // IT Manager, 2004. — № 15(3). — С. 23.

В. В. Хоролец,
менеджер ВЭД аудиторско-консалтингового
частного предприятия «Ависта»

УПРАВЛЕНИЕ СТОИМОСТЬЮ КОМПАНИИ: ОЦЕНКА И УПРАВЛЕНИЕ

Поиск решения проблем развития рыночной инфраструктуры во всем ее многообразии вызван тем, что остроту приобретает вопрос о том, сколько может стоить компания, предприятие, отдельный бизнес или его часть. Исходя из этого, целью статьи яв-